

AMANDA N. LISKAMM
Director, Consumer Protection Branch
SHEILA B. BERMAN
MANU J. SEBASTIAN
Trial Attorney
U.S. Department of Justice
Consumer Protection Branch
450 Fifth Street, NW, Suite 6400S
Washington, D.C. 20001
Telephone: (202) 307-0061
Facsimile: (202) 514-8742
Email: Sheila.B.Berman@usdoj.gov

E. MARTIN ESTRADA
United States Attorney
MACK E. JENKINS
Assistant United States Attorney
Chief, Criminal Division
VALERIE L. MAKAREWICZ (Cal. Bar No. 229637)
Assistant United States Attorney
Major Frauds Section
1100 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-0756
Facsimile: (213) 894-6269
E-mail: Valerie.Makarewicz@usdoj.gov

Attorneys for Plaintiff
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

No. 5:23-CR-00021-JGB

Plaintiff,

V.

JASON EDWARD THOMAS CARDIFF

GOVERNMENT'S MEMORANDUM OF POINTS
AND AUTHORITIES IN SUPPORT OF ITS
OPPOSITION TO MOTION TO DISMISS
COUNT TWO OF THE INDICTMENT

Date: October 21, 2024
Time: 2:00 p.m.
Courtroom: 1

Plaintiff United States of America, by and through its counsel of record, the United States Attorney for the Central District of California and Assistant United States Attorney Valerie L. Makarewicz

and Department of Justice Trial Attorneys Sheila B. Berman and Manu J. Sebastian, hereby respectfully files its Opposition to Defendant's Motion to Dismiss Count Two of the Indictment.

Dated September 23, 2024

Respectfully submitted,

AMANDA LISKAMM
Director
Consumer Protection Branch

E. MARTIN ESTRADA
United States Attorney

/s/
SHEILA B. BERMAN
MANU J. SEBASTIAN
Trial Attorneys
VALERIE L. MAKAREWICZ
Assistant United States Attorney

Attorneys for Plaintiff
United States of America

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	SUMMARY OF FACTS.....	2
III.	LEGAL STANDARDS AND ARGUMENT.....	4
A.	Standard for Dismissing Count Two of the Indictment.....	4
B.	Defendant's Motion to Dismiss Count 2 should be denied as use of the means of identification is at the crux of the predicate offense.....	5
C.	Security measures did not prevent Defendant from fraudulently using and transferring full credit card and debit card account numbers.....	8
D.	Aggravated Identity Theft is Not Limited to Situations Involving Impersonation.....	10
E.	Defendant's Fraudulent New Orders on Behalf of Former Customers Were Not Garden-Variety Overbilling.....	13
IV.	CONCLUSION.....	15

1
2 **TABLE OF AUTHORITIES**
3

	Page(s)
4 Cases	
5 <u>Dubin v. United States</u> , 6 599 U.S. 110 (2023)	passim
7 <u>Flores-Figueroa v. United States</u> , 8 556 U.S. 646 (2009)	13
9 <u>Hamling v. United States</u> , 10 418 U.S. 87 (1974)	4
11 <u>United States v. Boren</u> , 12 278 F.3d 911 (9th Cir. 2002)	5
13 <u>United States v. Carll</u> , 14 105 U.S. 611 (1882)	4
15 <u>United States v. Felch</u> , 16 No. 21-CR-0570, 2024 WL 406554 (D.N.M. Jan. 22, 2024)	12
17 <u>United States v. Gladden</u> , 18 78 F.4th 1232 (11th Cir. 2023)	12
19 <u>United States v. Harris</u> , 20 983 F.3d 1125 (9th Cir. 2020)	10
21 <u>United States v. Iannelli</u> , 22 700 F.Supp.3d 1 (D. Mass. 2023)	13
23 <u>United States v. Lyle</u> , 24 742 F.3d 434 (9th Cir. 2014)	5
25 <u>United States v. Michael</u> , 26 882 F.3d 624 (6th Cir. 2018)	11
27 <u>United States v. Ovsepian</u> , 28 No. 21-55515, 2024 WL 4020019 (9th Cir. 2024)	8
<u>United States v. Pernillo-Fuentes</u> , 252 F.3d 1030 (9th Cir. 2001)	4
<u>United States v. Shortt Accountancy Corp.</u> , 785 F.2d 1448 (9th Cir. 1986)	5

1 Statutes

2 18 U.S.C. § 2.....	1
3 18 U.S.C. § 1028A(a)(1).....	passim
4 18 U.S.C. § 1029(a)(5).....	1, 2, 6, 7
5 18 U.S.C. § 1347.....	5
6 18 U.S.C. § 1512(b)(2)(B).....	1
7	

8 Rules

9 Federal Rule of Criminal Procedure 12(b)(3)(B)(v).....	4
10	

1
MEMORANDUM OF POINTS AND AUTHORITIES
2

3 **I. INTRODUCTION**

4 On January 31, 2023, a federal grand jury returned the
5 Indictment against Defendant, charging him with access device fraud
6 in violation of 18 U.S.C. § 1029(a)(5) and 18 U.S.C. § 2 (Count One);
7 aggravated identity theft in violation of 18 U.S.C. § 1028A(a)(1) and
8 18 U.S.C. § 2 (Count Two); and two counts of witness tampering in
9 violation of 18 U.S.C. § 1512(b)(2)(B) (Counts Three and Four).
10 Indictment, Dkt.1.

11 Defendant has moved the Court to dismiss Count 2 of the
12 Indictment, aggravated identity theft in violation of 18 U.S.C. §
13 1028A(a)(1), in the wake of the Supreme Court's ruling in Dubin v.
14 United States, 599 U.S. 110 (2023). In Dubin, in light of a Circuit
15 split, the Supreme Court considered what constituted "use" of a means
16 of identification "in relation to" the predicate offense under 18
17 U.S.C. § 1028A(a)(1): a broad reading of the terms that would include
18 use of a means of identification that "facilitates or furthers the
19 predicate offense in some way" or a more targeted reading that
20 requires "a genuine nexus to the predicate offense." Dubin, 599 U.S.
21 at 116-117.

22 The Court held that 18 U.S.C. § 1028A(a)(1) "is violated when
23 the defendant's misuse of another person's means of identification is
24 at the crux of what makes the underlying offense criminal, rather
25 than merely an ancillary feature of a billing method." Id. at 114.

26 The facts of this case fall squarely within the Supreme Court's
27 ruling in Dubin, as the fraudulent use of victims' credit card and
28 debit card account numbers is an element of both crimes.

1 Specifically, as it relates to Count Two, during approximately
2 January 2018 through May 2018, Defendant ordered his employees to
3 participate in a scheme that defrauded former customers out of money
4 by misusing their credit and debit card account numbers and placing
5 them on periodic continuity plans without their authorization or
6 consent, thus charging those customers for products that they did not
7 order. Indictment, Dkt.1.

8 As relates to Count 1, the underlying offense of access device
9 fraud in violation of 18 U.S.C. § 1029(a)(5), Defendant is charged
10 with fraudulently using the same credit card and debit card account
11 numbers of those customers, which are access devices. Defendant's
12 fraudulent use of the credit card and debit card account numbers was
13 not ancillary to the predicate offense, but was part and parcel of
14 the charged criminal act.

15 **II. SUMMARY OF FACTS**

16 Defendant has accepted as true, for purposes of this motion, the
17 FTC's Statement of Uncontroverted Facts and Conclusions of Law, filed
18 in FTC v. Cardiff, et al., Case No. 5:18-CV-02104 (C.D. Cal. 2018) as
19 Dkt. No. 423-3, relevant portions of which are summarized below.
20 Defense Motion to Dismiss Count Two of the Indictment, Dkt. 106, n.2
21 (hereinafter "Def. Mot."). Beginning in January of 2018, Defendant
22 directed the staff at his company, Redwood, to create brand new
23 "continuity" (subscription) orders for customers who had previously
24 made "straight sale" (one-time) purchases, so their debit and credit
25 cards on file could be charged again and going forward on a recurring
26 basis. Defense Motion to Dismiss Count Two of the Indictment, Exhibit
27 A., Dkt. 106-1, p.6. (hereinafter "Def. Mot. Ex. A") No one at
28 Redwood contacted the affected consumers to get approval for the new

1 charges; Redwood staff processed hundreds of unauthorized
2 transactions each day. Id. at 7-8. Over time, the staff attempted to
3 place new continuity orders using customer information associated
4 with older and older straight sale orders, and ultimately attempted
5 to convert all 2017 straight sale orders into new continuity orders.
6 Id. at 9. Redwood processed unauthorized charges for more than 1,500
7 consumers through Defendant's straight-to-continuity initiative. Id.
8 Defendant set a revenue goal for staff of \$10,000 a day from the
9 straight-to-continuity initiative. Id. In some cases, former
10 customers' credit/ debit cards had expired since placing their
11 original order. Id. at 8. Defendant directed his employees to try
12 changing the expiration dates to new dates to facilitate the
13 processing of new unauthorized charges. Id.

14 Redwood used a business called Limelight, later known as
15 "Sticky.io" as its Customer Relationship Management provider
16 (hereinafter "The CRM"). Id. at 14. The CRM integrated third-party
17 providers into Redwood's system including the payment processors that
18 sent information from Redwood's website to banks for processing. Id.
19 Defendant and his employees were able to access information in the
20 CRM system, including billing names and addresses, shipping names and
21 addresses, and partial credit card numbers. Id. at 17, 21. The CRM
22 platform gave Defendant, and the employees he directed, the ability
23 to use a customer credit card "on file" to place a new order with the
24 click of a button. Id. at 15.

25 The mechanism used to create the fraudulent charges was to
26 submit a "new order card on file" transaction. Id. at 19. On January
27 22, 2018, Redwood employee Julie Green emailed Defendant and two
28 other employees step-by-step instructions on how Redwood could

1 process "new order card on file" transactions. Id. at 65, 72. There
2 were two slightly different sets of instructions sent out a few hours
3 apart; both directed the employee creating the new charge to work
4 from a spreadsheet containing prior single-sale orders, open the old
5 order of a single-sale customer, and "choose place a new order." Id.
6 CRM employee Joanny Spina confirmed that both sets of instructions
7 were ways to process new orders for a prior purchaser using the card
8 on file. Id. at 18-19. She identified one set of instructions as what
9 she would recommend using if a client had a straight sale customer
10 who requested to be put on continuity, but noted that that was not
11 common. Id. at 19. In reviewing a spreadsheet of former customers who
12 were placed on continuity, Spina indicated it was a time-consuming
13 process, saying it would take a lot of people to create new card on
14 file transactions for everyone on the list. Id. Notably, the CRM did
15 not require the logging of customer consent for new order card on
16 file transactions in 2018, although that changed in 2020 when the NMI
17 PaySafe payment processor began enforcing the requirement to document
18 customer consent for a new charge. Id. at 19.

19 **III. LEGAL STANDARDS AND ARGUMENT**

20 **A. Standard for Dismissing Count Two of the Indictment**

21 Under Federal Rule of Criminal Procedure 12(b)(3)(B)(v), a
22 defendant may move to dismiss a count in an indictment on the grounds
23 that the count "fail[s] to state an offense." Every count must "set
24 forth all the elements necessary to constitute the offence intended
25 to be punished." Hamling v. United States, 418 U.S. 87, 117 (1974)
26 (quoting United States v. Carll, 105 U.S. 611, 612 (1882)). Where a
27 count fails to recite an essential element of the offense, that count
28 is facially defective and must be dismissed. See United States v.

1 Pernillo-Fuentes, 252 F.3d 1030, 1032 (9th Cir. 2001).

2 For purposes of ruling on a motion to dismiss a count in an
3 indictment, courts are "bound by the four corners of the indictment."
4 United States v. Lyle, 742 F.3d 434, 436 (9th Cir. 2014) (quoting
5 United States v. Boren, 278 F.3d 911, 914 (9th Cir. 2002)). Courts
6 accept the allegations in the indictment as true and "analyz[e]
7 whether a cognizable offense has been charged." Boren, 278 F.3d at
8 914.

9 A motion to dismiss a count in an indictment can be determined
10 before trial if it presents legal, rather than factual, issues.

11 United States v. Shortt Accountancy Corp., 785 F.2d 1448, 1452 (9th
12 Cir. 1986).

13 **B. Defendant's Motion to Dismiss Count 2 should be denied as
14 use of the means of identification is at the crux of the
predicate offense.**

15 The aggravated identity theft charge in this case is proper
16 under the Supreme Court's recent decision in Dubin. At issue in Dubin
17 was whether the petitioner, who defrauded Medicaid in violation of 18
18 U.S.C. § 1347, also committed aggravated identity theft under §
19 1028A(a)(1). The Court's analysis focused on what constitutes "use"
20 of a means of identification "in relation to" the predicate offense.
21 Dubin, 599 U.S. at 116-117.

22 In Dubin, the Government advocated for a broad reading of the
23 terms, to include any use of a means of identification that
24 "facilitates or furthers the predicate offense in some way." Id. at
25 117. Petitioner advocated for a more targeted reading, where "the
26 means of identification is at the crux of what makes the predicate
27 offense criminal, rather than merely an ancillary feature of a
28 payment method." Id. The Court found the government's proposed

1 interpretation to be too broad a reading, as it would "apply
2 automatically any time a name or other means of identification was
3 part of a billing method used in commission of a long line of
4 predicate offenses." Id. (cleaned up). The Court found the more
5 targeted reading was correct, holding that "1028A(a)(1) is violated
6 when the defendant's misuse of another person's means of
7 identification is at the crux of what makes the underlying offense
8 criminal, rather than merely an ancillary feature of a billing
9 method." Id. at 114.

10 In Dubin, the Government charged aggravated identity theft for
11 use of a patient's Medicaid number on a claim submitted to Medicaid
12 for testing performed by a licensed psychologist, when the person who
13 actually performed the testing was a less-qualified licensed
14 psychological associate. Id. The qualification of the practitioner
15 dictated the amount of the fee paid, and the misrepresentation of the
16 practitioner as a licensed psychologist inflated the amount. Id. The
17 Court found "the crux of the healthcare fraud was a misrepresentation
18 about the qualifications of the petitioner's employee." Id. at 132.

19 The patient received the services in question and his means of
20 identification was not in and of itself used in a manner that was
21 fraudulent or deceptive. As the fraudulent act was misrepresenting
22 the qualification of the provider, misuse of the patient's means of
23 identification on a billing form was determined to be ancillary to
24 the crime.

25 Aggravated identity theft, 18 U.S.C. § 1028A(a)(1), prohibits
26 the knowing "transfer, possess[ion], or us[e], without lawful
27 authority, a means of identification of another person," during and
28 in relation to, among other offenses, access device fraud (18 U.S.C.

1 § 1029(a)(5)). 18 U.S.C. § 1028A(a)(1) & (c)(4).

2 In this case, the predicate offense to the government's charge
3 of aggravated identity theft is access device fraud in violation of
4 18 U.S.C. § 1029(a)(5), which prohibits, "knowingly and with intent
5 to defraud effect(ing) transactions with 1 or more access devices
6 issued to another person to receive payment . . . during any 1-year
7 period . . . equal to or greater than \$1,000." Defendant is charged
8 with fraudulently using former Redwood customers' access devices,
9 specifically their credit and debit card account numbers and
10 expiration dates, to effect financial transactions and obtain money.
11 Indictment, Dkt. 1.

12 The aggravated identity theft count charges Defendant with the
13 transfer, possession, and use, without lawful authority, of names and
14 credit and debit card account numbers during and in relation to the
15 commission of the access device fraud. Indictment, Dkt 1.

16 The credit and debit card account numbers referenced in both the
17 identity theft and access device counts are one and the same.
18 Defendant's use of the victims' names and credit card and debit card
19 account numbers is the first element of the predicate crime. The
20 relevant jury instruction is "First, "with [an access device] [access
21 devices] issued to [another person] [other persons] the defendant
22 knowingly effected transactions." Ninth Circuit Model Criminal Jury
23 Instruction 15.14 (2022 ed). Thus, for Count 2, Defendant's use of
24 the credit card and debit card account numbers of former customers
25 was not ancillary to the underlying charged criminal act, it was part
26 and parcel of the unlawful use of an access device offense.

27 While the Supreme Court acknowledges in Dubin that the "crux"
28 test may result in some difficult "close cases," 599 U.S. at n.10,

1 this is not one of them. A Venn diagram depicting the access devices
2 Defendant fraudulently used to effect transactions in violation of
3 §1029(a)(5) and the means of identification Defendant misused in
4 violation of 1028A(a)(1) would depict two heavily overlapping
5 circles, both of which contain the former customers' credit and debit
6 card account numbers. "Identity theft is committed when a defendant
7 uses the means of identification itself to defraud or deceive." Id.
8 at 123. That is exactly what happened in this case.

9 The Ovsepian case Defendant cites in support of his Motion to
10 Dismiss, presented facts that were "unusually narrow" and is not
11 instructive here. United States v. Ovsepian, No. 21-55515, 2024 WL
12 4020019 at *9-10 (9th Cir. 2024). There was no analysis or
13 consideration of the use or transfer of any means of identification
14 as the government made the strategic choice to focus on possession of
15 a single patient file onsite. The aggravated identity theft
16 conviction was overturned because possession of that file, which at
17 best "may have lent [the defendant] an air of legitimacy . . . to
18 survive an audit," was not at the crux of the conspiracy to commit
19 healthcare fraud. Id. at *10.

20 **C. Security measures did not prevent Defendant from
21 fraudulently using and transferring full credit card and
debit card account numbers**

22 "Identity theft covers both when someone steals personal
23 information about and belonging to another ... and uses the
24 information to deceive others," and "fraudulent appropriation and
25 use." Dubin, 599 U.S. at 126 (emphasis in original) (cleaned up).
26 "Identity theft thus intermingles aspects of theft and fraud,
27 misappropriation and deceitful use." Id. at 126-127. "Section
28 1028A(a)(1)'s three verbs capture this complexity." Id. at 127. While

1 "transfer" and "possess" conjure up two steps of theft, "uses"
2 supplies the deceitful use aspect. Id.

3 Defendant went to great lengths describing how the CRM system
4 encrypts and protects credit card and debit card numbers so that they
5 are not fully transparent to either Redwood or CRM personnel. Def.
6 Mot. 4-6. There is no dispute that only partial credit card and debit
7 card numbers were visible to Redwood staff and CRM staff, and the
8 full numbers were "securely tokenized and securitized" in the CRM
9 computer system. Id.

10 While the ability to see the full credit card or debit card
11 number might arguably be relevant to a charge based solely on
12 possession of an account number as a means of identification, that is
13 not the allegation here. Defendant offers no case law or statutory
14 provision in support of the position that direct possession of each
15 digit of a credit or debit card account number is necessary in order
16 to misuse the full number or transfer it to another entity for
17 payment without authorization.

18 Defendant also asserts that as a result of the security measures
19 there was no "unauthorized access or misuse" of customers' cards
20 simply because the full credit card and debit card numbers account
21 were "never accessible to anyone within Redwood." Id. at 6. That
22 statement is simply not true; the credit and debit card numbers of
23 over 1,500 former customers were misused to make unauthorized
24 purchases.

25 Defendant has acknowledged the actual use of the credit card and
26 debit card account numbers as part of his straight-to-continuity
27 initiative. "While using those customers' names and credit and debit
28 card numbers was necessary to charge them for the subscriptions, that

1 causal relationship is not sufficient under Dubin." Id. at 11-12
2 (emphasis added). The card owners did not place orders for new
3 subscription plans. Defendant ordered his staff to place the new
4 orders, and they did so without getting the cardholders'
5 authorization. Defendant was able to bypass the protections meant to
6 secure the credit card and debit card account numbers from fraudulent
7 use by placing "new order card on file" transactions using the full
8 card numbers on file. In 2018, there was no requirement by the
9 payment processor to record customer consent in order to process
10 these transactions. Enforcement of the customer consent requirements
11 in 2020 suggests recognition by the payment processors that they
12 needed to close the loophole that allowed sellers like Defendant to
13 commit fraud by creating "new order card on file" transactions
14 without customer consent. Unfortunately, it came too late to help
15 protect the fraud victims in this case.

16 In creating "new order card on file" transactions, Defendant was
17 able to use the full card account number, which was transferred from
18 Redwood's computer ordering system, through the payment processor to
19 the financial institutions that charged the unwitting former
20 customers' for the "purchase" of new products. The fact that the
21 charges went through is evidence that the full account numbers were
22 used as means of identification without lawful authority.

23 **D. Aggravated Identity Theft is Not Limited to Situations
24 Involving Impersonation**

25 "Use" of a means of identification in an aggravated identity
26 theft case is not limited to cases of "impersonation" where the
27 defendant assumes an individual's identity or attempts to pass
28 themselves off as another. United States v. Harris, 983 F.3d 1125 (9th

1 Cir. 2020); see also United States v. Michael, 882 F.3d 624 (6th
2 Cir. 2018) (reversed the trial court's dismissal of an aggravated
3 identity theft count that was granted on the grounds it did not
4 involve impersonation.)

5 Based on construction of the statutory language in 18 U.S.C.
6 § 1028A(a)(1), the grammatical object of "use" is a "means of
7 identification" and therefore "use" in this context means, "[t]o
8 convert to one's service" or "to employ" the means of
9 identification." Webster's New International Dictionary 2806 (2d ed.
10 1942). See United States v. Michael, 882 F.3d 624, 626 (6th Cir.
11 2018). "Use" can also be defined as "[t]o put (an instrument,
12 implement, etc.) to practical use; esp. to make use of (a device
13 designed for the purpose) in accomplishing a task"). Id. at 626;
14 Black's Law Dictionary 1776 (10th ed. 2014). There is nothing within
15 the statutory language that "suggests 'uses' refers only to assuming
16 an identity or passing oneself off as a particular person." Id. at
17 627.

18 Defendant appears to take the position that Count 2 should be
19 dismissed on the theory that there was no effort by Defendant to pass
20 himself off as another person or misrepresent his identity. Def. Mot.
21 at 10-11, 13. The argument relies on a somewhat difficult to follow
22 "who" framing of the question and the assertion that, "There *must* be
23 deception going to 'who' is involved in the transaction rather than
24 just 'how' or 'when' services were provided." Def. Mot. at 10.
25 (emphasis added).

26 In Dubin, the Supreme Court identifies the "who" framing, as a
27 heuristic, or rule of thumb, that can be helpful in determining if
28 the means of identification is used deceptively and therefore at the

1 locus or crux of the predicate criminal activity, but also noted
2 "that like any rule of thumb it will have its limits." Dubin, 599
3 U.S. at 132. The "who" construction does not replace the "crux"
4 analysis to determine if a means of identification is used in
5 relation to the underlying offense.

6 "[F]or fraud or deceit crimes like the one in this case, the
7 means of identification specifically must be used in a manner that is
8 fraudulent or deceptive. Such fraud or deceit going to identity can
9 often be succinctly summarized as going to 'who' is involved."
10 Dubin, 599 U.S. at 131-132.

11 Although Dubin "redirects the statute's focus to offenses built
12 around what the defendant does with the means of identification in
13 particular, § 1028A still proscribes uses of a means of
14 identification involving fraud and deceit about identity." United
15 States v. Felch, No. 21-CR-0570, 2024 WL 406554, at *2 (D.N.M. Jan.
16 22, 2024) citing United States v. Gladden, 78 F.4th 1232, 1244 (11th
17 Cir. 2023) (cleaned up). This includes fraud and deceit as to "who"
18 authorized payment of funds.

19 In Felch, the defendant used, a means of identification,
20 specifically her employer's signature on a check, representing that
21 the authorized signatory on the account had approved payment of funds
22 when he had not. Id. "Ms. Felch's fraudulent use of her employer's
23 signature can be succinctly summarized as going to who was involved
24 in the authorization of the check." Id. at *2. "[U]se of her
25 employer's identity to falsely represent to the bank that the check
26 she wrote . . . was authorized by her employer remains firmly at the
27 crux of the predicate bank fraud charge." Id. at 4.

28 A bookkeeper's use of a signature stamp she was generally

1 authorized to use on an unauthorized check she wrote to herself was a
2 misrepresentation of "who" authorized the withdrawal of funds.

3 United States v. Iannelli, 700 F.Supp.3d 1, 3 (D. Mass. 2023). "Such
4 misrepresentation is at the crux of the alleged bank fraud because by
5 whom the signature on a check is authorized determines who is liable
6 for the face amount of the check." Id.

7 Here, Defendant's fraudulent transactions involved deception as
8 to 'who' was involved in approving the transaction and not simply
9 'how' or 'when' services were rendered. Defendant had his staff
10 submit self-dealing "purchases," without the card owners' knowledge
11 or authorization. On the face of the each of the fraudulent
12 transactions, it appeared that the victim cardholder had authorized
13 payment for a product sold by Defendant's company. In fact, the
14 victims had not purchased a product or authorized a payment and did
15 not have knowledge that their cards were being charged. Defendant's
16 employees had simply accessed credit and debit card numbers stored in
17 a database from earlier transactions and used those means of
18 identification to fraudulently obtain cash directly from the
19 cardholder's bank account (debit card) or credit card company. This
20 is a classic form of identity theft "involving fraud or deceit about
21 identity: a defendant [who] has used another person's identification
22 information to get access to that person's bank account." Dubin, 599
23 U.S. at 126 (citing Flores-Figueroa v. United States, 556 U.S. 646 at
24 656 (2009)).

25 **E. Defendant's Fraudulent New Orders on Behalf of Former
26 Customers Were Not Garden-Variety Overbilling**

27 In Dubin, the Supreme Court did not hold that use of means of
28 identification for billing, even garden-variety billing, could not

1 support a violation of § 1028A(a)(1) if it is at the crux of the
2 predicate offense. Rather, the Court rejected a broad reading of the
3 relevant statutory language in part because, "the Government's
4 reading would, in practice, place garden-variety overbilling *at the*
5 *core* of §1028A(a)(1)." Dubin, 599 U.S. at 122 (emphasis added).

6 Defendant asks this Court to dismiss Count 2 of the Indictment
7 as the "alleged conduct was the type of 'garden variety' overbilling
8 that the Supreme Court held was not penalized by the statute." Def.
9 Mot. at 1.

10 Defendant's actions were not "garden-variety" overbilling.
11 Defendant placed wholly fraudulently orders and processed them for
12 payment. To overbill is "to submit a bill of charges to someone for
13 an amount in excess of what is due: to bill for an excessive amount."
14 *Overbill*, Merriam-Webster.com Dictionary, Merriam-Webster,
15 <https://www.merriam-webster.com/dictionary/overbill> (last visited
16 September 13, 2024). The examples of garden-variety overbilling
17 referenced in Dubin, a lawyer charging a client for 3 hours when only
18 2.9 hours of work was performed or a waiter serving flank steak and
19 charging for filet mignon, are excess charges on an otherwise
20 legitimate bill. Dubin, 599 U.S. at 113. In those scenarios, the
21 client hired the lawyer to do legal work and the diner ordered and
22 received a steak.

23 Here, the former customers did not place new orders, did not
24 request new products, and did not agree to pay for new products. They
25 were not charged more than what was due, as nothing was rightly due
26 and no legitimate bill existed. The actions of Defendant were not any
27 variety of overbilling—they were outright identity theft designed to
28 take money from the victims without their knowledge or authorization.

1
2 **IV. CONCLUSION**

3 For the reasons set forth herein, the government respectfully
4 requests the Court deny Defendant's Motion to Dismiss Count Two.
5

6 Dated September 23, 2024

Respectfully submitted,

8 E. MARTIN ESTRADA
United States Attorney
9

10 AMANDA LISKAMM
Director, Consumer Protection
11 Branch

12 /s/
13 _____
14 SHEILA B. BERMAN
15 MANU J. SEBASTIAN
Trial Attorney
VALERIE L. MAKAREWICZ
16 Assistant United States Attorney

17 Attorneys for Plaintiff
18 UNITED STATES OF AMERICA
19
20
21
22
23
24
25
26
27
28